BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Goodman et al.	Before the Examiner: Chai, Longbit
Serial No.: 09/931,629	Group Art Unit: 2131
Filing Date: August 16, 2001	
Title: FLASH UPDATE USING A TRUSTED PLATFORM MODULE	Lenovo (United States) Inc. ZHHA/B675/B424 P.O. 12195 3039 Cornwallis Road Research Triangle Park, NC 27709

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I. REAL PARTY IN INTEREST

Lenovo (Singapore) Pte. Ltd. is the assignee of the entire right, title and interest in the above-identified patent application.

CERTIFICATION UNDER 37 C.F.R. §1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on 5-7, 2006.

Signature

Toni Stanley
(Printed name of person certifying)

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, Appellants' legal representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal, except that Appellants filed an appeal of the rejections of the claims in U.S. Patent Application Serial No. 09/931,550, which is the subject of the provisional double patenting rejection in this Application.

III. STATUS OF CLAIMS

Claims 1-4 and 6-10 are pending in the Application. Claims 1-4 and 6-10 stand rejected.

IV. STATUS OF AMENDMENTS

Appellants have not submitted any amendments following receipt of the final rejection with a mailing date of September 20, 2005.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is described with respect to the update of a BIOS image within a data processing system, such as system 313. However, the present invention is applicable to the update of any data and/or image within an information handling system. [Page 8, lines 18-20]

The present invention makes use of the TCPA (Trusted Computing Platform Alliance) Specification where a trusted platform module (TPM) 351 has been installed within system 313. *See* FIGURE 3. The TCPA Specification is published at www.trustedpc.org/home/home.htm, which is hereby incorporated by reference herein. However, it should be noted that the present invention may also be implemented using other cryptographic verification methods and processes. [Page 8, line 21 – page 9, line 2]

Referring to FIGURE 1, system 313, either automatically, or as a result of input from a user, will begin a process where the BIOS image is to be updated. Such a BIOS image may reside within ROM 316 or some other memory module within system 313. [Page 9, lines 3-5]

Referring to FIGURE 1, in step 101, a BIOS update application will run on system 313 and will request signature verification of a newly received BIOS image from the TPM 351. This launches the process illustrated in FIGURE 2 wherein step 201, the TPM receives the verification request from the BIOS update application and performs a signature verification on the update utility and the updated BIOS image. The TPM 351 may utilize a signature verification process that is a standard method that is used in many cryptographic systems. The sender of the BIOS image computes a "hash" of the original work (a hash is a mathematical computation that is performed on the input; the computation is designed such that the probability of being able to recreate the output without the identical input is low). Then the hash is encrypted using the sender's private key. This encrypted result is called the signature. When the receiver, the TPM 351, wishes to verify that the image is authentic, the TPM 351 computes the hash of what was received. The TPM 351 then decrypts the sender's signature by using the sender's public key and compares it to the newly computed hash. If they are identical, the TPM 351 then determines that the update image is authentic and has not been modified in transit. [Page 9, lines 7-21]

If in step 202 (FIGURE 2) the verification resulted in a successful verification of the BIOS utility and image, the process proceeds to step 203 where the TPM 351 unlocks the flash memory using various methods, such as a general purpose output pin on the TPM 351. In step 204, the TPM 351 will post that it has completed a successful verification to the BIOS update application. [Page 10, lines 6-10]

Returning to step 103, if the verification was successful, then the process proceeds to step 106 where the BIOS update application updates the BIOS image, and

unlocks the flash memory. Locking the flash memory can be performed by a request to the TPM 351 to perform the locking process. [Page 10, lines 11-17]

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 4 and 8 stand provisionally rejected under the judicial created doctrine of obviousness-type double patenting as being unpatentable over claim 18 (and claim 3) of co-pending Application Serial No. 09/931,550.

2. Claims 1-4 and 6-10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Alexander et al.* (U.S. Patent No. 6,188,602) in view of *Grawrock* (U.S. Patent No. 6,678,833).

VII. ARGUMENTS

1. Claims 1, 4 and 8 stand provisionally rejected under the judicial created doctrine of obviousness-type double patenting as being unpatentable over claim 18 (and claim 3) of co-pending Application Serial No. 09/931,550. In response, Applicants respectfully traverse this rejection, however, since the co-pending application is merely pending, Applicants will address this double patenting rejection when either such co-pending application issues or claims 1, 4 and 8 are allowed in this Application.

2. Claims 1-4 and 6-10 stand rejected under 35 U.S.C. § 103 as being unpatentable over *Alexander* (U.S. Patent No. 6,188,602), in view of *Grawrock* (U.S. Patent No. 6,678,833). In response, Applicants respectfully traverse these rejections.

The claims recite that a TPM performs a signature verification of an update to a program, such as a BIOS image recited in certain claims. If this signature verification is successful, then the TPM unlocks a memory unit to store the program.

In Applicants' previous response of July 15, 2005 (which is incorporated herein), Applicants argued, and Examiner has not apparently disagreed, that *Grawrock* does not teach a TPM performing a signature verification of an update to

the program. *Grawrock* stores the updated program and then performs a TPM verification.

In response, the Examiner has replied that *Alexander* was actually relied upon by the Examiner to address such claim limitations. However, *Alexander* does not teach what the Examiner asserts. Referring to Fig. 3A of *Alexander*, *Alexander* teaches that the flash memory 212 enters state 330 where flash memory 212 in firmware hub 110 is reset to read/write access. Column 5, lines 32-34. Flash memory 212 then enters state 332 to check whether there is a valid RBU image to update BIOS 142. Column 5, lines 34-36. If a valid RBU image exists, flash memory 212 enters state 338 where BIOS 142 updates firmware hub 110 with a new BIOS image and then enters state 302 to load the new image by resetting computer system 100. Column 5, lines 41-45.

In state 330, the flash memory is reset to a read/write access. This is the same as unlocking the flash memory. The Examiner is respectfully requested to refer to the attached Declaration by Steve Goodman, who is attesting to such an assertion. Thereafter, in state 332, then *Alexander* checks whether the RBU image is valid. This is opposite of what the Examiner is asserting.

As a result, both *Alexander* and *Grawrock* both specifically teach that the flash memory is unlocked before the program is updated. Thus, the combination of *Alexander* and *Grawrock* would install an update to the program, and thereafter verify the program. This is the opposite of what is recited in the claims.

As a result, the combination of *Alexander* and *Grawrock* teaches away from the present invention. As a result, the Examiner has failed to prove a *prima facie* case of obviousness in rejecting the claims.

The citation by the Examiner (in the Advisory Action) to Column 3, lines 62-64 fails to support his position. This language is taken out of context; it has no connection to the description in Column 5.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Appellants

By: _____

Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2832

CLAIMS APPENDIX

1. A method for updating a program in a data processing system comprising the steps of:

requesting a trusted platform module ("TPM") to perform a signature verification of an update to the program;

the TPM performing the signature verification of the update to the program;

if the signature verification of the update to the program is successful, using the TPM for unlocking a memory unit storing the program; and

modifying the program with the update to the program in response to the unlocking of the memory unit storing the program.

2. The method as recited in claim 1, further comprising the step of:

locking the memory unit after the modifying step.

3. The method as recited in claim 2, wherein the locking step is performed by the TPM.

4. A computer program product for storage on a computer readable medium and operable for updating a BIOS stored in a flash memory in a data processing system, comprising:

a BIOS update application program receiving an updated BIOS image;

the BIOS update application requesting a TPM to perform a signature verification of the updated BIOS image;

a TPM program receiving the request from the BIOS update application to perform the signature verification of the updated BIOS image;

the TPM program performing the signature verification of the updated BIOS image and posting a result of the signature verification of the updated BIOS image to the BIOS update application;

if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks the flash memory; and

the BIOS update application modifies the BIOS with the updated BIOS image.

6. The computer program product as recited in claim 4, further comprising:

programming for locking the flash memory after the BIOS update application modifies the BIOS with the updated BIOS image.

7. The computer program product as recited in claim 6, further comprising:

if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is not authentic, then an error message is output.

8. A data processing system having circuitry for updating a BIOS stored in a flash memory in the data processing system, comprising:

input circuitry for receiving an updated BIOS image;

circuitry for requesting a TPM to perform a signature verification of the updated BIOS image;

the TPM performing the signature verification of the updated BIOS image;

the TPM unlocking the flash memory if the signature verification of the updated BIOS image determines that the updated BIOS image is authentic; and

circuitry for modifying the BIOS with the updated BIOS image.

9. The system as recited in claim 8, further comprising:

circuitry for locking the flash memory after the BIOS is modified with the updated BIOS image.

10. The system as recited in claim 8, further comprising:

circuitry for outputting an error if the signature verification of the updated BIOS image determines that the updated BIOS image is not authentic.

EVIDENCE APPENDIX

A declaration under 37 C.F.R. § 1.132 by Steve Goodman is relied upon by Appellants in the appeal, a copy of which is attached.

RELATED PROCEEDINGS APPENDIX

Co-pending U.S. Patent Application Serial No. 09/931,550 has also been appealed by Appellants. That Application is relied upon by the Examiner in his provisional double patenting rejection.

In re Application of: Goodman et al.	:	Before the Examiner: Longbit Chai
Serial No.: 09/931,629	:	Group Art Unit: 2131
Filed: August 16, 2001	:	Lenovo (United States), Inc.
Title: FLASH UPDATE USING A TRUSTED PLATFORM MODULE	:	Intellectual Property Law ZHHA/B675/B424 P.O. Box 12195 3039 Cornwallis Road Research Triangle Park, NC 27709

DECLARATION UNDER 37 C.F.R. § 1.132

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

I, Steve Goodman, am an inventor of the above-identified Application, and declare as follows:

Setting flash memory in firmware to read/write access is equivalent to unlocking the flash memory.

CERTIFICATION UNDER 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on 10-20, 2005.

Toni Stanley
Signature

Toni Stanley
(Printed name of person certifying)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this Declaration is directed.

By: _____
Steve D. Goodman

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2851